SAIC's Enterprise Security Solutions

Controlling SPAM

Doug Andre, CISSP, SSCP

September, 2003

Agenda

- What is SPAM?
- Definition of SPAM
- Spammer Come-Ons
- So What’s the Problem?
- Additional SPAM Issues
- How do Spammers get Addresses?
- Closing the Door on SPAM

What is SPAM?

- Spam is difficult to define. In fact, there is no clear definition.
  - Is it SPAM if it tries to sell you something?
  - Is pornography SPAM?
  - Are personal jokes from friends considered SPAM?
  - Unsolicited political messages?
- We all recognize SPAM when we see it, but the truth is that what is SPAM to one person may not be SPAM to another. An e-mail that is considered SPAM at work may not be considered SPAM at home.

Definition of SPAM

- There is no definition that is universally accepted.
- The most prevalent definition seems to be the term “unsolicited commercial e-mail” (UCE).
  - UCE is any commercial electronic mail message that is sent often in bulk, to a consumer without the consumer’s prior request or consent.

SPAMMER Come-Ons

- This is a one time mailing, you may be removed from future mailing by replying to the above address thank you.

- ***Our research indicates that the following material may be of interest to you; (However, so that we may be courteous, please reply by email with the word 'remove' to be immediately removed from further mailings. You must type 'remove'.)

- THIS IS NOT SPAM! The mailing list used was purchased from a broker and sold as a webmasters list. We were told that you have requested news related to the marketplace. If this is NOT true, (we sincerely apologize for the intrusion) please send an e-mail to: feedback@bannercash.net and ask to be removed. YOU WILL NOT RECIEVE ANY MORE E-MAIL!

So What's the Problem?

- A recent study by the Radicati Group estimated that a company with 10,000 employees not employing SPAM fighting techniques will spend $49 per user on server resources to handle SPAM.
- Compared to an average of $25 per user for those companies employing SPAM fighting techniques.
- Estimated server costs will rise to $257 per user by 2007.

Additional SPAM Issues

- SPAM is no longer just a nuisance but quickly becoming a potential legal liability and productivity drain for corporate IT departments and users alike.
- SPAM is also another conduit for unknown viral applications into the corporation, for links to pornographic or objectionable Web sites, and for leaks of sensitive company information. For these reasons SPAM not only place strain on corporate bandwidth and storage, it creates legal pitfalls too.

How do SPAMMERs get addresses?

- Spiders or robot programs.
- SPAM replies.
- Signing up for free stuff.
- Internet Yellow and White pages.
- Email servers.
- Hacking.
- Guessing.
- DNS registries.

Closing the Door on SPAM

No one has the perfect solution to fight SPAM!

- **Fighting SPAM should be done as a multi-layered effort.**
- **The following will be addressed in further detail regarding a multi-layered approach:**
  - **Legislation**
  - **Open Relays**
  - **Technical Anti-SPAM Techniques**
    - **Pros and Cons**
  - **User Anti-SPAM Techniques**

Legislation

- There are currently no enacted Federal laws against SPAM. However, 29 states have passed laws that regulate SPAM, including Maryland.

- In Maryland's anti-SPAM law, commercial e-mail messages that use third party domain names without permission, that contain false or missing routing information, or have false or misleading subject lines are illegal.
- The law applies if messages are sent from Maryland, if the sender knows that the recipient is a Maryland resident, or if the owner of the domain name found in the recipient's address will confirm that the recipient is a Maryland resident.

Open Relays

- The settings of your mail server may make your system vulnerable to misuse if it maintains an “open relay” to the Internet.
- Open relays are configured to accept and transfer email on behalf of any user anywhere, thus allowing any e-mail sender anywhere to pass messages through the server and onto the ultimate recipient.
- Spammers scan the Internet looking for “open relays”.
- “Open relays” allow Spammers to route their bulk email through that server, thus Spamming in in greater volume and less time all the while concealing their identities.

Technical Anti-SPAM Techniques

TECHNIQUE	PROs	CONs
<u>Keyword Filtering</u>: Specific strings are searched for in an e-mail message.	Simple to implement. Already available in many e-mail packages.	Not very accurate. Frequent false positives (Good e-mail messages tagged as SPAM)
<u>Rule-Based Filtering</u>: E-mail messages are filtered and scored by keyword and context using a set of rules.	Can be very accurate.	Requires ongoing rule updating. May miss well crafted SPAM messages.

Technical Anti-SPAM Techniques

TECHNIQUE	PROs	CONs
Bayesian Filtering: A type of statistical analysis derived from Bayesian logic.	Learns to recognize SPAM. Returns percentage probabilities instead of scores. Can be very accurate.	Depends somewhat on the quality of SPAM used to teach it. May need to be customized for each user.
Blacklists: Lists of IP addresses that have been identified to originate SPAM.	Good at blocking known SPAM resources.	Requires constant updating. Misses well crafted SPAM messages and SPAM that isn't coming from known mail relays.

Technical Anti-SPAM Techniques

TECHNIQUE	PROs	CONs
Fingerprinting: Identification of SPAM based on similarity to previously received SPAM messages.	Can quickly recognize SPAM with a high rate of accuracy.	Doesn’t recognize new SPAM messages. Requires constant updating from a central source.
Challenge-Response: E-mail senders are challenged to prove their identity before e-mail messages are delivered.	Very high degree of SPAM prevention.	Creates more e-mail traffic. May block valid e-mail sent by machines. May require foreign language support.

Technical Anti-SPAM Techniques

TECHNIQUE	PROs	CONs
Secure Messaging: E-mail is sent with encrypted credentials or on an encrypted transport, so that the sender or sending machine can be authenticated.	Very high degree of SPAM prevention. Reliable identification of e-mail source.	Requires widespread acceptance and support for digital identity standards. May require expensive infrastructure enhancements.

User Anti-SPAM Techniques

- Consider “masking” or “munging” your e-mail address
  - yourname@example-REMOVE_THIS-.com
- Set up disposable addresses
- Use two e-mail accounts
- Try not to display your e-mail address in public
- Check privacy policy before you submit your address to a website
- Read and understand the entire form before you transmit personal information through a website
- Use an email filter
- Use a unique email address

Helpful Resources

- Federal Trade Commission
  - http://www.ftc.gov/spam
- SpamAssassin
  - http://spamassassin.rediris.es/index.html
- Stop-SPAM.org
  - http://www.stop-spam.org
- Coalition Against Unsolicited Commercial Email
  - http://www.cauce.org
- SPAM Abuse
  - http://spam.abuse.net

SAIC's Enterprise Security Solutions

Thank You